BLACK WALLET
RISK INDICATORS REPORT

POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

Polisen
Swedish Police

BLACK WALLET
RISK INDICATORS REPORT

The Black Wallet Project is funded by the European Union's Internal Security Fund - Police. The content of this document represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Table of Contents

List of Abbreviations

AML	Anti-money Laundering
ATM	Automated Teller Machine
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
FATF	Financial Action Task Force
Fintech	Financial Technology
FIU	Financial Intelligence Unit
IOCTA	Internet Organized Crime Threat Assessment
KYC	Know Your Customer
NGO	Non-Governmental Organization
ML	Money Laundering
PEP	Politically Exposed Person
PSP	Payment Service Provider
STR	Suspicious Transaction Report
TF	Terrorist Financing

Glossary

FIAT money	Currency established as money, often by government regulation
Front man	”A person of no means,” or one who deliberately accepts a liability or other monetary responsibility without the resources to fulfill it

Preface

The Black Wallet Project is an EU-funded, joint project between the Finnish and Swedish Financial Intelligence Units (FIUs) with support from other competent authorities from the respective countries. During the course of the project (March 2019 to February 2021), the aim has been to create an overall picture of the Fintech (Financial Technology) sector, especially focusing on products and services related to the transferring of funds. Ultimately, this has helped the law enforcement authorities and the private sector to prevent, detect and investigate Money Laundering and Terrorist Financing (ML/TF).

This report is a part of the Black Wallet Project's risk indicators end product. The report accompanies the Risk Indicators, which are targeted to Payment Service Providers (PSPs) and Fintech companies in order to help the companies realize, assess and mitigate risks that may arise in relation to their products and services. The report provides detailed information and examples of threats, vulnerabilities and red flags that the Black Wallet Project Group has identified in relation to the Fintech sector.

The first chapter of the report presents risk assessments conducted by different supranational entities, such as the Financial Action Task Force and the European Banking Authority, which the Black Wallet Project Group has utilized while compiling the risk indicators. In addition to the supranational entities' risk assessments, the Project Group has utilized risk indicator listings and risk assessments conducted by different FIUs within the European Union (EU). Therefore, we want to thank all the FIUs who have contributed to create this risk assessment specifically focusing on the Fintech sector.

The following chapters focus on the risks that are relevant to the Fintech sector. The threats, vulnerabilities and red flags relevant to the Fintech sector have been identified by analyzing the aforementioned supranational risks assessments, the risk assessments conducted by FIUs within the EU and the input received from the companies participating in the Black Wallet Project.

The Black Wallet Risk Indicators is not a scoring system, which means that it does not take into account the severity of different risks. Furthermore, it does not provide recommendations about what type of mitigation measures should be taken. The sole purpose of the risk indicators is to highlight possible risks in order to help PSP's to identify risks relevant to their business, to evaluate the severity of each risk and to assess appropriate preventive measures to prevent the realization of the identified risks.

Lastly, it should be noted that the Risk Indicators produced by the Black Wallet Project does not cover all the possible risk scenarios. Therefore, the companies should consider other possible risks when creating and updating their own risk assessments and mitigation measures.

Money Laundering and Terrorist Financing Risk Assessments

To aid the development of the Black Wallet Project Risk Indicators, the Project Group familiarized with several risk assessments conducted by supranational organizations and national entities that are active within the European Union (EU). It was quickly noticed that there is no coherent risk assessment methodology and that entities categorize ML and TF risks differently. The risk assessments that the Project Group has surveyed are briefly described in the following chapters.

European Banking Authority Risk Factor Guidelines

The European Banking Authority (EBA) Risk Factor Guidelines[1] were adopted in June 2015 as a result of the EU Directive 2015/849. The Directive aims to harmonize EU legislation with the International Standards on Combating Money Laundering and Terror Financing and Proliferation adopted by the FATF (Financial Action Task Force) in 2012. The EU Directive 2015/849 is in line with the FATF standards, which focus on a risk-based approach in combating ML and TF.

The EBA guidelines set out factors that companies should consider when assessing ML/TF risks. The guidelines provide tools for companies to adjust their customer due diligence to correspond with the identified risks. However, the EBA points out that the measures described in the report are not exhaustive and that companies should take other factors and measures into account as well.

The guidelines are divided into three parts:

- **Title I** sets out the subject matter, scope and definition of the guidelines.
- **Title II** focuses on assessing and managing general risks. The aim is to give companies tools to make risk-based decisions when identifying, assessing and managing ML/TF-associated risks.
- **Title III** provides sector-specific guidelines and sets out risk factors that are of particular importance for certain sectors.

According to the guideline **Title II**, risk assessments should consist of two distinct, but related steps:

1. **The identification of ML/TF risk**
   Identifying risk factors from various sources of information, such as the EU Commission's supranational risk assessment, regulators, national risk assessments, FIUs and from the companies' own CDD processes. The guideline also includes lists of different risk factors, which have been categorized as followed: customer risk factors, countries and geographical areas, products, services and transactions, risk factors, and delivery channel risk factors.
2. **The assessment of ML/TF risk**
   After identifying the risks, the guideline encourages companies to take a holistic view of ML/TF risk factors and to weigh some of the factors differently depending on their relative importance.

Title III provides sector-specific guidance to correspondent banks, retail banks, electronic money issuers, money remitters and investment firms, among others. The guidelines conclude with accompanying documents, such as an impact assessment, which describes the policy options that the EBA considered when drafting the guidelines.

[1] European Banking Authority, Final Guidelines, 26.6.2017.
https://eba.europa.eu/sites/default/documents/files/documents/10180/1890686/66ec16d9-0c02-428b-a294-ad1e3d659e70/Final%20Guidelines%20on%20Risk%20Factors%20(JC%202017%2037).pdf

Financial Action Task Force

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against ML, TF and financing of the proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter financing of terrorism (CFT) standards. The Project Group surveyed two risk assessments by the FATF: The National Money Laundering and Terrorist Financing Risk Assessment[2] and The Terrorist Financing Risk Assessment Guidance[3].

National Money Laundering and Terrorist Financing Risk Assessment

The National Money Laundering and Terrorist Financing Risk Assessment provides guidance for countries in conducting risk assessments on a national level. The principles described in the Risk Assessment are also relevant to more focused risk assessments, such as a particular financial sector.

The Risk Assessment has the following structure:

Section 1 sets out the purpose, scope and status of the Risk Assessment.

Section 2 includes general principles that should be taken into account when conducting ML/TF risk assessments.

- Clear agreement on purpose
- Determining the scope
- Level of commitment of the process

Section 3 is about planning and organizing ML/TF risk assessment on a national level. For instance it gives examples of different authorities that countries should consider cooperating with in the assessment process. The section also discusses the involvement of the private sector and other actors.

Section 4 presents the three main stages involved in the risk assessment process:

1. **Identification**, which begins by developing a list of potential risks or risk factors that countries face when combating ML/TF. The identified risks will be drawn from suspected threats or vulnerabilities.
2. **Analysis**, which is in the heart of the assessment process. This includes consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, the aim of this stage is to gain a holistic understanding of each risk – as a combination of threats, vulnerability and consequence – in order to work towards assigning some relative value or importance to them.
3. **Evaluation**, which means determining the priorities of the previously analyzed risks for addressing them. These priorities may contribute to the development of strategy or risk mitigating measures.

Section 5 shortly describes how the outcome of the risk assessment can be presented.

Terrorist Financing Risk Assessment Guidance

The Terrorist Financing Risk Assessment Guidance aims to assist practitioners, particularly in low-capacity countries, in assessing terrorist financing risks at the jurisdiction level by providing good approaches, relevant information sources and practical examples based on country experience.

[2] Financial Action Task Force,
National Money Laundering and Terrorist Financing Risk Assessment, 2013.
https://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

[3] Financial Action Task Force, Terrorist Financing Risk Assessment Guidance, 2019.
https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf

The report addresses:

- Key considerations when determining the relevant scope and governance of a terrorist financing risk assessment, as well as practical examples of how to overcome information-sharing challenges related to terrorism and its financing.
- Examples of information sources when identifying threats and vulnerabilities related to terrorist financing, and different considerations within specific national contexts (e.g. financial and trade centers, lower capacity jurisdictions, jurisdictions bordering conflict zones etc.).
- Relevant information sources when identifying cross-border terrorist financing risks and terrorist financing risks within banking and money or value transfer sectors, as well as addressing non-profit organizations that fall within the FATF definition.
- Good approaches for maintaining up-to-date assessments of risks and areas of further consideration.

Europol Internet Organized Crime Threat Assessment

Europol's European Cybercrime Centre (EC3) annually publishes an Internet Organized Crime Threat Assessment (IOCTA)[4], which is the main strategic report on key findings and emerging threats and developments in cybercrime, as well as threats against governments, businesses and citizens in the EU. The IOCTA provides key recommendations to law enforcement agencies, policy makers and regulators with the aim of improving the effectiveness of cybercrime responses. IOCTA focuses on crime areas that fall under the EC3's mandate, which currently are

- Cyber-dependent crime
- Online child sexual exploitation
- Payment fraud

The IOCTA 2019 also focuses on online criminal markets, both on the surface web and the Darknet, and addresses the convergence of cyber and terrorism.

The IOCTA report's main findings regarding payment fraud focus on card fraud, skimming and jackpotting. One form of jackpotting is the Black Box attack, which is performed by cashing out ATMs. The latest IOCTA also mentions the report from 2017, which addressed the risk that instant payments could complicate fraud prevention and, particularly, mitigation. Since 2017, various different instant payment schemes have been launched that have inevitably provided benefits for the financial sector in terms of providing new ways of making payments. However, new instant payment schemes have also inadvertently provided money launderers with more options for money mule accounts and making it harder for the financial sector to block suspicious transactions, among others. One of the key recommendations made by the IOCTA 2019 for tackling payment fraud is to enhance cooperation between and within the public and private sector.

European Commission Supranational Risk Assessment

A report from the Commission[5] to the European Parliament and the Council on the assessment of the risk of ML and TF affecting the internal market and relating to cross-border activities was published on 24.7.2019. The report provides a systematic analysis of ML and TF risks related to specific products and services. It focuses on vulnerabilities identified within the EU, both in terms of the legal framework, as well as effective applications, and provides recommendations for addressing them.

[4] Europol, Internet Organized Crime Threat Assessment, 2019. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

[5] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 2019. https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf

The Supranational Risk Assessment identifies 47 products and services within 11 sectors, which are potentially vulnerable to risks associated with ML and TF. The main risks identified in the report include:

- Cash and cash-like assets
- Financial sub-sectors, such as foreign exchange offices, transfers of funds and e-money products
- Non-financial sectors, such as manufacturers, distributors and legal professionals, where main weakness appears to be the inability to identify client's beneficial owner
- Gambling sector
- Collection of transfers of funds through non-profit organizations

New products/sectors:

- Professional football
- Free ports
- Investor citizenships and residence schemes

The report identifies horizontal vulnerabilities that are common to all sectors, which are the following:

- Anonymity in financial transactions
- Identification and access to beneficial ownership information
- Supervision in the internal market
- Cooperation between FIUs
- Infiltration by criminals
- Forgery
- Insufficient information sharing between the public and private sectors
- Insufficient resources, risk awareness and know-hows
- Risks emerging from Fintech

In addition, the report provides a list of how to mitigate these risks through EU policy, as well as recommendations for supervisory authorities and member states.

Risk Indicators by the FIUs in the EU

The Black Wallet Project Group contacted FIUs in the EU and requested risk indicators created by the FIU or law enforcement authorities that focused on ML/TF. The received risk indicators were subsequently utilized as a source for creating the Black Wallet Risk Indicators.

Black Wallet Risk Indicators

Since the launch of the Black Wallet Project in March 2019, the Project Group has been collecting data and information in order to develop the risk indicators. This chapter describes the method used to create the most relevant indicators for the project's target group, PSPs and Fintech companies.

Online Survey

The results of the Black Wallet online survey were one of the main sources of the Black Wallet Risk Indicators. The Project Group started drafting the online survey in July 2019. Several people from different law enforcement agencies, such as the Finnish and Swedish FIUs, the FIN-FSA and the Finnish Security and Intelligence Service participated in creating the survey. A select number of Finnish and Swedish target group companies also gave valuable feedback while drafting the survey.

The survey included questions about company information, product and service information, transaction information, Know Your Customer (KYC) and monitoring, as well as legal information. It was disseminated in the fall 2019 to companies that fell within the scope of the project. These companies were PSPs and other Fintech companies. In the project's scope, PSP is perceived as the general and top-level definition, which refers to Fintech companies offering a payment service of some kind. Other or related Fintech companies that did not necessarily offer a method of payment, were defined as entities that provided an accompanying service to PSPs.

Some of these Fintech companies are obliged entities and some are not. For instance, an example of the accompanying service can be a company who conducts KYC processes on behalf of the PSP. The participating companies in the scope of the project were registered in an EU country or in the United Kingdom and provided services to Finland and Sweden.

In total, the Project Group identified 1088 companies that matched the scope of the project and provided services to Finland and Sweden. The companies were identified by using different company listings from Fintech associations, the Nordic Tech Database, the European Banking Authority and Financial Supervisory Authorities. In addition to the lists, the Project Group also used open source searches to identify target group companies.

An invitation to participate in the project and to answer the online survey was sent to 301 companies of which 91 companies replied. The answers given by companies helped identify threats, vulnerabilities and red flags that entities in the Fintech sector might face and should try to mitigate within the framework of their operations.

Project Group Meetings

The Project Group for the Black Wallet Project consisted of people working at different law enforcement agencies in Finland and Sweden. From October 2019, the Project Group worked together to create the risk indicators.

The Project Group met on a regular basis to discuss the risk indicators in order to ensure that the findings from the online survey replies were firmly grounded in a common understanding, as well as to make sure that all points of view were taken into account in the end product. The meetings consisted of face-to-face workshops, video conferences, as well as email correspondence between the Project Group members.

After closing the online survey, the Project Group held the first risk indicator workshop during which the answers were analyzed and potential risk factors were identified based on the responses that the target group companies had provided regarding their products and services. Based on the survey responses, the Project Group members looked for Fintech sector-specific risks from ML and TF perspective. The work process consisted of both identifying the risks highlighted by the respondents, as well as identifying any missing methods or risky behaviours. It was observed that several companies already had ML and TF mitigation practices in place and had comprehensively considered how to implement KYC and monitoring practices in their daily activities. However, some companies lacked adequate methods.

After reviewing the material, the Project Group established the following three risk themes that were specific to the sector:

- **Risks related to the sporadic nature of the services**. These include, for example, the fragmentation of data when multiple parties are involved in a single transaction and outsourcing parts of a service to third party operators.
- **Risks related to the management of customer information**. The Project Group identified that the target companies often relied on other sources when it came to KYC processes or customer identification, among others. Furthermore, the majority of the target group companies operated online and client accounts were set up digitally, which makes modifications of the account information easier.
- **Miscellaneous risks**. For example, this includes the lack of a risk assessment related to money laundering, static transaction monitoring limits or fixed monitoring and the use of cloud services.

These three themes provided a foundation for assessing the sector-specific risks of the Fintech industry.

After the first workshop in October 2019, the Project Group met on a regular basis to create a methodology for the indicators. The Project Group analyzed the risk indicators conducted by other entities and FIUs to create a methodology that was understandable and comprehensive, and that was compatible with the Fintech industry and the companies' products and services. The Project Group also paid close attention to creating examples of each risk in the final product. This was done in order to provide the companies with examples of real events in which a specific risk could take place and to support the analysis of each risk in the different categories. The examples can be found under each risk category described later in this report.

In-depth Analysis of the Survey Results, Risk Categories

In addition to the Project Group meetings, an analyst from the Finnish FIU analyzed the survey results quantitatively and qualitatively. One section of the analysis presents the relevant risks that the target companies see in their products and services.

The survey respondents were asked to provide a free-text description of the ML/TF risks they had identified or considered relevant for their business. 15 survey participants (16.5% of total) opted not to respond. Of the remaining 76 participants, nine companies stated that they did not conduct their own risk assessment, which was conducted by a business partner or a customer instead. Some companies also stated that they had not identified any significant ML/TF risks.

Based on the general trends observed in the free-text responses of the survey, it was possible to formulate the following five general ML/TF-related risk categories:

- Products and services
- Processes and systems used in KYC or customer identification
- Customer or client risk
- Geographical location
- Personnel / employee risk

The Project Group took these risk categories into account when formulating the risk assessment. The different categories formulated based on the survey answers can be seen in the final product, the Black Wallet Risk Indicators.

Methodology of the Black Wallet Risk Indicators

After assessing different entities' risk indicators and assessments, the Project Group decided to use a similar method as the FATF uses to categorize risks and alter the categories to cover PSPs, Fintechs and their supportive services. The Risk Indicators move from the broader threats to more specific vulnerabilities and finally to red flags, which the companies can flag in their products and transactions.

In FATF methodology threat means people, object or activity with the potential to cause harm. In Black Wallet Risk Indicators, the assumption is that Fintechs and PSPs attract criminals. Therefore, threats in Black Wallet Risk Indicators cover events and features that are relevant and common to the Fintech industry, rather than the people, object or activity from which the threat emerge. Fintech payment industry is relatively young without a seasoned mindset of crime prevention and cooperation with authorities and the companies are often small and offer quick, cross border services. One may argue that there are threats concerning the capabilities of the Fintech payment companies to follow the legislative obligations and capabilities to monitor and report complex and fragmented transactions. In Black Wallet Risk Indicators, threats cover the top level events and features that can be common to the whole industry. Threats can also be perceived as something that the companies may have limited ability to control with their risk mitigation measures. Threats are sprung from the playing field of the companies, such as obligations set by local or transnational authorities or the way customers use the products and services.

The Black Wallet Risk Indicators' perspective on vulnerabilities is almost similar to FATF's, which takes into account the features of a particular sector or a financial product. In Black Wallet Risk Indicators, vulnerabilities are characteristics in the PSPs themselves and in their connected or supportive services. The PSPs have the power to mitigate vulnerabilities to some extent by planning business operations and developing their products accordingly.

In addition to threats and vulnerabilities, FATF has a concept of consequence, which refers to the impact or harm that ML or TF may cause. This is important, but more in place in the national risk assessments. For this reason, in the Black Wallet Risk Indicators this concept was replaced with a practical level of red flags, which concern the risks derived from the customers and from their behaviour. Red flags in the Black Wallet Risk Indicators encompass registering and KYC, customer profile and transactions.

The following chapters present the Black Wallet Risk Indicators risk categories in more detail. The aim is to support the risk indicators by providing a detailed explanation of each risk category and different risks with tangible, real life examples.

Threats

Threats in the Black Wallet Risk Indicators cover the top level events and features common to the whole industry. Threats can be perceived as something that the companies have limited ability to control, and the source and nature may vary over time. Threats may emerge from criminal activity seeking to exploit the vulnerabilities in the industry. Therefore, it is important to consider the environment in which both the threats and the industry function. The threat analysis of Black Wallet therefore looks at threats as the playing field of the companies, such as obligations set by local and transnational authorities or the way customers use the products and services.

Compliance and Legal Obligations

Threats stemming from compliance and legal obligations consist of challenges within the PSP and the judicial authorities in the jurisdiction that the PSP is registered at. For instance, in regards to compliance within the PSP, the PSP may face challenges in collecting relevant information about their customers, which affects their ability to identify customer specific risks. Customer risks, such the service being used for illicit purposes, are inevitable and should therefore be consciously tackled.

The reason why a PSP has inadequate compliance mechanisms may be due to the lack of staff or relevant technical abilities. This has an effect on the PSP's ability to monitor their customers thoroughly, which in turn has an effect on the suspicious transaction reports that the company submits to the local FIU. Without proper customer identification, KYC and monitoring, the PSP is not fully aware of its customers' behaviour, including the regular behaviour of the customer. As a result, the PSP is unable identify suspicious or deviant activities.

PSPs have a legal obligation to ensure that their employees receive adequate training regarding AML and CFT measures in order accurately perform their duties. A lack of knowledge caused by PSPs not providing adequate training can result as a significant employee risks. In practice, this could lead to a situation where the PSP employees are not familiar with the relevant risk indicators and are therefore not able to identify risks or suspicious actions. In addition, a small number of employees may be a risk factor, if this translates to insufficient resources.

Lastly, significant issues may arise if the company lacks risk awareness and adequate risk assessments of the PSP itself. This could be due to the prevailing PSP mind-set, which predominantly focuses on innovation rather than risks. The PSPs may also be unaware of their own playing field, which could lead them into thinking that their service would not be used for illicit purposes.

Fintech Service Specific Features

Fintech companies are known for their ability to provide fast transaction services in multiple geographical locations through online platforms or applications, among others. These characteristics of the sector give rise to sector-specific threats that PSPs should be aware of and take into consideration when developing and implementing risk mitigation measures.

The payer or payee may be located in an area or state with higher ML/TF risk than the jurisdiction in which the PSP that provides the service is registered. For instance, high-risk area or state may lack developed, formal banking sector, which means that informal remittance services, such as hawalas, may be more prevalent as a payment method.

Furthermore, PSPs' customers may receive funds from sources in a state associated with higher ML/TF risk. It is important that Fintech companies pay particular attention to geographical locations known to provide funding or support terrorist activities or where groups committing terrorist offences are known to be operating. This applies to states and jurisdictions subject to financial sanctions, embargoes or preventative measures against terrorism, financing of terrorism or proliferation.

Fast, complex and high-volume transactions are also Fintech sector-specific features. Speed and complexity of the transaction chain is important to keep in mind when assessing risks related to PSPs. Questions such as who the middle men are (intermediary PSPs in the transaction), what customer or transaction information PSP can see and whether the PSP has an obligation to report suspicious activity are important to take into consideration. The complexity of the transactions can also affect the authority's ability to identify who the actual sender or receiver of the funds is.

Transparency and Traceability of the Transaction

Transparency and traceability of the transaction refer to the PSP's ability to identify how the transaction data is separated, what data different actors that are part of the transaction hold and who are the actors to which the PSP has outsourced part of their service. For example, the separation of data may hamper the obligation to report if important information remains in the hands of an entity that is not obliged to report suspicious transactions. The fragmentation of information can also put PSPs in a situation where none of the actors in the transaction chain have the full picture of the customer and his or hers behaviour.

Illicit Purpose of the Company

If PSPs are established for illicit purposes, it clearly leads to a heightened risk of ML/TF. Notwithstanding, PSPs that are established for legitimate purposes can knowingly or unknowingly be funded by illicit sources, which enables the criminal funder to acquire more control of the company.

Authorities

The identified threats also have significant implications for the authorities. If authorities are unaware or do not understand the nature of different the Fintech services PSPs, it leads to a lack of understanding of the flow of transactions. This is connected to the complexity of transactions, which occurs through different types of accounts. For instance, customer funds accounts may not be directly connected to a natural person and may involve multiple PSPs in the transaction chain, which makes it difficult to follow the flow of funds.

Additional difficulty in tracing the flow of funds stems from the cross-border and instantaneous nature of Fintech services. For example, a PSP in one EU country may offer services to a PSP in another member state. This may lead to a situation in which data regarding customers operations can only be acquired from the PSP's domicile country or (if different) from the country in which the PSP is located at.

As a result of the international nature of the Fintech services, there may be several jurisdictions connected to one transaction. Thus, cross-border services increase the need for requesting information from the authorities or directly from the service providers in another jurisdiction. Requesting information from authorities in other jurisdictions can take a long time and cause significant delays in the investigative processes.

Furthermore, simple inquiries to services providers in another country can be burdensome, since often the correct contact details are unavailable or the service provider refuses to reply. However, it should be noted that a service provider could potentially find it difficult to distinguish between a legitimate authority request and, for example, a phishing attempt.

The identified issues can have a significant effect on the capabilities of the authorities' as they often require the verification of the identity of the payer and payee, as well as the traceability of assets in their operations.

In practice, the competent supervisory and investigative authorities, such as FIUs and other law enforcement agencies, are facing the same issues in their own operations, including registering, licensing, supervising and investigating these services. This is by no means to be understood as the service provider's fault, as it is the authority's responsibility to keep up with the technical development.

Lastly, it can be argued that the threats that the authorities, as well as the service providers, face require a deeper and closer public-private partnerships in Europe than what has been conducted so far.

Vulnerabilities

Vulnerabilities are the second level of risks in the Black Wallet Risk Indicators. Vulnerabilities are characteristics in the PSPs themselves and in their connected or supportive services. Vulnerabilities are divided into three categories: The first category is product, which consists of risks related to the PSP's products. The second category is distribution channel, which consists of risks related to the ways how transactions for example are carried out. Lastly, the third category is PSP's own traits and functions, which are risks related to the nature of the PSP and how its operations are carried out. The PSPs have the power to mitigate vulnerabilities to some extent by planning business operations and developing their products accordingly.

The following sub-chapters present the three different categories of vulnerabilities with various risk examples for each category.

Product

Vulnerabilities in products are related to the allocation and availability of products to customers, as well as the usage of the product.

High-value activities create risks when there are no adequate thresholds for transactions, payments, storing, loading or redemption, including withdrawals. For example, the lack of adequate thresholds can potentially allow customers to move large sums of funds for illicit purposes or move funds by making large transactions or large payments. Furthermore, products can be loaded with large sums in one country and cashed out in another country.

This situation is similar to moving cash from one country to another, with the difference that using a cross-border instant service or transporting funds in a prepaid instrument, makes the transport of funds easier and faster. Funding the product, that is, placing funds to be used by the product, can be done anonymously with cash, e-money, exemption granted e-money products that do not require KYC such as low value prepaid cards, or by unidentified third parties. For example, the product can be funded directly with cash, without KYC in place. This could potentially create a situation in which a customer can make a cash deposit in a store or at an ATM accepting cash, convert the cash to an electronic form and enable the customer to use the deposited funds. The customer can also fund the products by using a prepaid card, which means that the customer places its prepaid card details into another e-money product. Funding the product can also consist of payments from unidentified third parties. As such, this means that the product can be funded by persons or entities who have not done the KYC procedures or that their KYC information is not conveyed to the PSP offering the product.

Risks always exist when the use of the product allows person-to-person transfers, as they enable quick and easy transfers for illicit purposes. Arguably, more risks occur if the transfers can be done cross-border, especially to and from countries that are known to be high risk in terms of ML or TF.

If the product is suitable for services that pose a high risk and is known to be used for financial crime, such as online gambling, a risk is always present. Risks also occur if the product or service has a global reach, is used in cross-border transactions in different jurisdictions or if other people than the customer can use the product.

The issue of multiple people using the same product may occur in relation to the emission of business credit cards.

The possibility of changing customer information without proper KYC generates a risk of customer anonymity. Therefore, if the process of changing user account information lacks proper safeguards, it also potentially creates a risk in relation to the product. For instance, without proper safeguards in place, the PSP may not realize that the user of a service is constantly changing certain customer information in order to conceal the illicit use of the product.

Distribution Channel

The risks related to the second category of vulnerabilities, distribution channel, consist of risks related to the ways in which the transactions are carried out.

If the PSP utilizes customer funds accounts without following EU regulations on wire transfers[6], it can create anonymity and complexity issues. In practice, this can create a situation in which the customer data does not accompany the transaction, thereby securing higher anonymity for the user. Since the funds are deposited and travel through a customer funds account held by the PSP, there will be more levels in the payment chain. In practice, the money will travel from the payer's bank account to the PSP's bank account, which is held by a credit institution, and finally to the payee.

A higher level of complexity occurs if the PSP uses another PSP for certain transfers. In this case, the money travels from the payer's bank account to PSP's bank account, which is held by a credit institution, to another PSP's bank account, which is held by another credit institution, and finally to the payee. An alternate payment scenario is that the initial source of funds is something other than a bank account, such as a prepaid payment card.

Distribution channels can also provide a degree of anonymity for the customer, for example when prepaid cards are sold without customer identification procedures. In this situation, the PSP has a limited amount or no information about the customer or the user of their product.

Providing the service exclusively online without adequate safeguards creates a risk due to the wide accessibility of the product, as well as the ability to make quick transactions. Risks also occur if the service is provided through agents that have unusual turnover patterns compared to agents in similar locations.

This includes unusually high or low transaction sizes, unusually large cash transactions, a high number of transactions that fall just under the customer due diligence threshold and operation of business outside of normal business hours. This could be relevant in situations where agents accept suspicious cash deposits, do not conduct KYC, or advise or encourage the payee to make payments under customer due diligence thresholds and transfer them electronically.

The service may potentially be provided through agents that undertake a large portion of business with payers or payees from jurisdictions associated with a higher ML/TF risk. These agents may have inconsistent AML/CFT policies, not come from the financial sector or conduct another business than their main business.

Providing services through a large network of agents in different jurisdictions or through intermediaries who are not obliged entities is also a risk in the distribution channel that companies should be aware of. All of these factors should encourage the primary PSP to pay close attention to its agent network.

[6] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

For example, if the primary PSP has a license to provide services to 30 different countries and use an agent network to offer the service, the PSP should pay attention if an agent specialises in offering the service to a high-risk area.

Risks in the distribution channels also include data security and data handling, especially if the data is secured or stored using third party service provider. The European Banking Authority has released instructions on best-practice cloud outsourcing for organisations that advise financial institutions to adopt a risk-based approach by implementing adequate controls and measures to ensure that third-party cloud provider relationships adhere to regulations.

A risk also arises if the PSP is connected to several service providers that operate independently without proper coordination. For instance, PSP may not receive the relevant information from its third-party service providers, who are responsible for conducting KYC or monitoring transactions. PSPs may potentially consider the KYC of other actors within the transaction chain (e.g. the customer's bank) to be sufficient. Thus, any weaknesses within the chain of dependency could weaken the whole process. The use of non-official intermediaries that lack documentation or official webpages also pose a risk for the service providing company.

The segmentation of services, which is the provision of services by multiple service providers that operate independently without due oversight and coordination, is an acute and common risk for all PSPs. PSPs may not receive relevant information from third parties that are responsible for conducting the KYC or transaction monitoring. This leads to the PSP lacking essential and relevant customer information, which could be important for filling out suspicious transaction reports to the local FIU.

Payment Service Provider's Own Traits and Functions

A PSP's own traits and functions refers to the nature of the service, how the business is constructed, how the company is funded and what kind of sources the company utilizes to support its business.

Firstly, PSPs can be a very useful tool for criminals. For instance, perpetrators can use PSPs to channel illegal funds while simultaneously offering services to real and legitimate customers. This would mean that legal and illegal funds become mixed in the PSP. In practice, criminals could try to fund an existing PSP with the purpose of acquiring the majority of the shares, thereby gaining control of the company.

This could be connected to the practice of intentional hiding the PSP's ultimate beneficiary by using a front man. Even though this is not a common occurrence, this type of criminal intervention should still be taken into account as a real possibility at the executive level of the PSP.

Possessing limited information of customers, relying on the first phase of identification instead of constantly updating KYC information and not having face-to-face meetings with customers are all relevant risks that may have impact the company's ability to combat ML/TF. Overall, the result of insufficient customer information is that companies lack the customer categorization needed to mitigate and monitor risks. The aforementioned risks are especially relevant in services that are digital in nature and take place online.

Trusting unreliable sources or unknown companies may also form a risk from the perspective of ML/TF, including instance when the KYC process is outsourced to an unreliable or unknown business partner.

As a result, during the identification process, the information is checked and run through sources that are not reliable or that allow customers to update their customer information themselves. There also exists a level of trust between PSPs, banks and credit card companies in knowing their customers and monitoring their behavior. Furthermore, outsourcing raises a problem regarding the fragmentation of data between different companies, not only in KYC processes but also in other processes such as outsourced monitoring processes.

A lack of proper transaction monitoring is a significant risk that PSPs should take into account in their mitigation measures. Intentional or unintentional delayed monitoring facilitates the approval of illegal transactions, which makes it harder for authorities to stop funds that have been transferred due to criminal offenses, such as extortion or fraud.

Exclusively using static and fixed limits in monitoring prevents the PSP from detecting new patterns of criminal activities that the PSP's products might have been utilized for. Lastly, neglecting the capacity of PSPs to detect complex transaction patterns and customer relationships makes it easier for criminals to take an advantage of the PSP's services.

Red Flags

The third and final level of risks in the Black Wallet Risk Indicators is red flags. Red flags are the risks in the behaviour of the PSP's customers, cover registering and KYC, customer profile and transactions. Registering and KYC refer to risks during the registration or while conducting KYC. Red flags related to the customer's profile are linked to the customer behaviour that differs from regular product or service usage or indicates other abnormality compared to the intended use. Transaction red flags relate to transactions that customers initiate.

The following sub-chapters present the three different categories of red flags with detailed examples of each of the category.

Registering and KYC

Red flags can be indicated by a customer's actions, such as purchasing or using multiple e-money products from the same issuer at once or at the same time. The same applies if the customer frequently reloads the provided product or makes several transfers in a short period of time without a financially viable rationale. This behavior could be an indication that the customer is a front man and is acquiring e-money products for criminals who wish to hide their identities. It could also indicate that the customer transfers funds for illegal purposes.

An obvious red flag is when the product appears to be used by multiple people despite being designed to only be used by one registered customer. This can be the case if the product is used from several IP-addresses at the same time. In this scenario, the customer could be a front man who has acquired a payment method with the intention to be used by multiple people. The action could also indicate identity theft. In other words, that criminals have used a stolen identity to acquire a payment product or that a customer's payment method has been acquired by hackers and is sold on darknet and later used by other criminals.

Frequent changes in the customer identification data, such as information about the customer's home address, email, phone number, IP address or linked bank accounts can also raise suspicion. It can indicate a situation in which the registered customer is not the real user of the service. The examples described in the previous paragraph also apply to this red flag; the customer could be a front man, the action might indicate identity theft or the customer's payment method might have been acquired for criminal purposes.

If the product is not used for the purpose it was intended for, it could also indicate that someone other than the actual customer has acquired the product. A deviant use of the product could occur in situations where a product that is normally marketed for a specific group, for instance towards kids, is used in a place that is designed for adults, such as nightclubs.

In addition, a red flag may occur if the customer owns or operates a business that handles large amounts of cash. Since cash is anonymous, a customer could attempt to transfer funds into prepaid cards or deposit them into a payment account and then transfer the funds for illegal purposes.

A customer could also use a PSP to convert cash into a more usable form, such as a credit/debit card. Another example of a red flag related to the KYC process arises when a PSP's customer's business has a complicated ownership structure, since it could facilitate a situation in which the ultimate beneficiaries are tried to be hidden.

If customer's needs are better serviced elsewhere, for instance if a PSP is not local to the customer or its business, the possibility of red flags should be taken into account. In other words, a PSP may not be suitable for a customer or fit the customer's profile. This could indicate a situation in which the customer believes to have found a weakness in the PSP's KYC or monitoring methods and therefore uses the PSP in order to successfully transfer funds for illegal purposes.

When a customer appears to be acting on behalf of someone else or acts contrary to financially viable behavior, there is a red flag of ML or TF. This type of behavior can be detected if there are other people monitor the customer's actions or if the customer reads instructions from a note during a meeting with the PSP. When a customer's behaviour does not make any sense from a financial perspective, he or she may accepts poor exchange rates or high transaction charges without questioning the prices or requests a transaction in a currency that is not commonly used in the jurisdiction where the customer and/or recipient is located. Therefore, PSPs should be alerted, if a customer's use of their service is unusual.

Discrepancies in a customer's knowledge about the payee or incoming transactions are red flags that companies should take into account. If an incoming transaction is not accompanied with the required information about the payer or payee, it should be perceived as abnormal. In addition, transaction amounts are relevant if, for example, the amount sent or received is inconsistent with the customer's declared or expected financial situation. This might indicate that the customer is being forced or is willingly transferring funds on behalf of someone else. If the customer is unable to provide sufficient information about the origin of the received funds, it might be an indication of criminal activities as the customer could be trying to hide illegally obtained funds.

Red flag arises if the incoming transaction is not accompanied by the required information of the payer or payee. For example, if a PSP does not receive information about the final destination in the payment chain, it cannot fulfil its AML obligations. It also prevents it from identifying more complex payment patterns.

Inconsistencies and deviancies that arise during the customer registration process are also red flags that should be taken into account. If the registration is carried out using an anonymous or disposable email service, it could indicate that a customer wants to stay anonymous or use multiple accounts or services to transfer funds. It could also have been done in order to avoid transaction limits. A customer's contact information may be linked to multiple profiles, which indicates that the customer uses aliases or front men.

This type of behavior could be an indication of a money laundering network. If a customer's IP address and residential address are a mismatch, it could be an indication of fraud. However, it is important to note that the person could be visiting another country, be a frequent traveler or be using a VPN service.

Finally, another red flag arises if the customer is a Politically Exposed Person (PEP) is listed on a sanctions list, on an official freezing list or another publicly available list. Negative or contradictory publicity of the customer are also indicators that should be a cause of concern for companies.

Customer Profile

Red flags related to customer profile refer to abnormalities in a customer's behavior that can be identified by monitoring the transactions, product usage or background of a customer. In many of the red flag examples connected to customer profiles, the information that a customer has given to the company during the identification and KYC process contradicts with the customer's actions.

Inquiries about sum limits or other product or service restrictions could indicate a situation in which a customer is trying to avoid enhanced customer due diligence or safeguard an illegal payment. A deviant customer profile compared to the broader clientele of the company is also a factor that should be taken into account.

Another red flag is if the customer operates during outside of regular working hours, especially in relation to the traits of the customer. For example, an elderly person using Fintech payment solutions to buy a boat from another country in the middle of the night indicates an abnormality.

If a customer has connections with high-risk countries, sanctioned countries and/or tax havens or is politically exposed, exerts influence or has sanctions, there is a possibility that the customer is avoiding taxes or laundering money. Politically exposed people have the power to influence the public and may be approached and influenced by actors that conduct illegal activities. If a PEP misuses his/her position, it leads to corruption.

This type of behavior can be identified if the product usage does not match the customer profile. Connections with high-risk countries or nearby conflict areas without a valid or apparent reason should be red flagged with possible links to terrorist financing. A similar level of caution should be taken in situations where a customer has connections to organized crime groups or other criminal activities, since the customer could be acting on behalf of a criminal organization.

The use of a front man as a beneficial owner is always an indication of possible criminal activities. This is indicated by as a discrepancy in the information that the customer has given versus who the physical person that attends eventual face-to-face meetings with the PSP.

A customer requesting transaction documents to be sent to a different address than its profile, opening multiple accounts, possibly under different names, or using unusual IP address are additional red flags. The aforementioned examples may indicate that the customer wants to cover or hide its activities and identity. If the customer refuses or is unable to confirm the actual beneficiaries of transactions or if the client behavior analysis indicates abnormality and makes no financial sense, this constitutes another red flag in terms of ML and TF.

Transactions

The final category of red flags is risks related to transactions. This chapter provides examples of different events that may constitute a risk that should be taken into consideration when monitoring customer behaviour.

Transactions made close to or below the thresholds, which have no apparent financial rationale or legal purpose and are unusually high or complex, may indicate ML/TF. Unusual transactions compared to a customer's regular behavior, in combination with the information obtained during the KYC, could potentially indicate that the customer is acting as a front man. Taken together, the transactions do not meet the client's declared nature of business or usage of the service. If the account is repeatedly credited and debited without a valid

purpose, this could indicate that the user of the account is making multiple payments to the same payee in order in order to avoid potential one-time payment thresholds.

The registration of a new customer followed by a large volume of transactions within a short period of time may indicate that the user is trying to maximize the amount of funds being transferred or paid. A large volume of transactions just below the threshold further supports this assumption. This could be linked to identity theft, in which the actual user is different from the identity that has been provided to the PSP.

Situations in which several payers are connected to a single payee without any apparent reason could indicate that the payee is collecting payments from multiple payers, or vice versa. This type of funding mechanism could be used for illegal purposes. Another indicator of illicit purposes is if the funds are transferred through different payment accounts in order to obscure the origin of the funds.

Quick movement of funds to or from virtual currency platforms is a red flag that should be carefully monitored, as it potentially indicates that the origin of funds is being obfuscated by converting them into virtual currency and later into FIAT money.

Another indication ML or TF red flag is when customers make transactions under different names and addresses from the same IP address. This may also be the case when a customer resides in one country but uses a foreign IP address without a reasonable explanation.

An odd use of bill payment services, including the sums or usage purpose, may also be an indication of ML or TF. For example, the use of bill payment services could enable trade-based ML. In this scenario, the customer subscribes to products without paying, sells the products and transfers profits for illegal purposes. Using bill payment services can also enable purchases without strong customer identification, which facilitates the use of a false identity (possibly acquired via identity theft) for subscriptions.

Situations in which a customer transfers funds to an account to which donations are made or instructs all the funds to be deposited into a third party's account may indicate a red flag.

Domestic customers using foreign accounts may indicate illicit purposes, especially if there is no apparent economic sense for this kind of activity. For example, if a customer is young and travels a lot, it could make sense to use a foreign service suitable for making payments abroad. However, the rationale behind a person that never travels using the same service would not be as obvious and could indicate a risk.

The use of instant-purchasing services or instant transfers of large sums could indicate a red flag. For example, normally customers spend time browsing products before a purchase. If the user seems to just click and purchase as many expensive products as possible, it indicates that the transaction is the goal. This is not normal behavior and could indicate illegal activity.

A large volume of withdrawals within a short period of time could indicate a situation where the account is being cashed out as quickly as possible. For example, this could mean that someone is desperately transferring funds for illegal purposes and trying to maximize the amount of transferred funds.

Links to safe havens should be noted as an indication of possible illegal activity, since the purpose of the transfers may be to move funds beyond the reach of local authorities to geographical areas

where hiding illegal profits is easier. Furthermore, links to sanction lists, official freezing lists and other public lists should be red flagged, considering that a certain level of severity in the conduct is required to be put on these lists.

Another indication of possible ML/TF is links to specific individuals or countries, including connections to high-risk countries, individuals in high-risk countries, members of organized criminal groups and PEPs. In particular, links to PEPs in foreign countries should be noted as a red flag as it is possible that criminal actors exerting influence over the politically influential persons. In addition, connections to countries with a high risk for drug-related crime should be red flagged by the PSP.

Transactions with links to non-profit and non-governmental organizations (NGOs), especially in conflict zones, may be a red flag. This red flag is particularly acute in relation to TF, since terrorist organizations may cover their activity by acting as NGOs in order to receive donations or funds from abroad for illegal purposes. Purchasing goods or a combination of goods that can be used for illicit purposes may also indicate a TF risk.

Conclusion

As discussed throughout the paper, numerous risks of ML/TF arise in conjunction with Fintech services and products, specifically those of PSPs. Even though PSPs cannot mitigate the threats discussed in this paper on their own, it is unquestionable that there are issues that PSPs should be aware of. That being said, if PSPs become aware of the most common vulnerabilities in their services, they can contribute to the mitigation of risks by planning their operations and products accordingly. Red flags can be incorporated into extensive customer due diligence, as well as customer and transaction monitoring. Furthermore, proper KYC measures and monitoring are directly linked to qualitative suspicious transaction reports (STRs) that are sent to local FIUs. By sending high quality STRs to local FIUs, PSPs can be involved in and contribute to revealing suspicious behavior and consequently tackle ML/TF.

The ambition of Black Wallet Project is that these risk indicators can be a starting point for tackling the risk of Fintech services and products being used for ML/TF purposes, by giving PSPs better tools to detect suspicious actions in order to generate high-quality reports to FIUs. As such, the purpose of the report and the Risk Assessment Chart is to provide PSPs with tangible examples and descriptions of the identified risks in order to figure out the relevant risks in their products and services.

Looking ahead, the Black Wallet Project Group finds that the public-private partnership between PSPs and FIUs within the EU needs to be enhanced. Since Fintech services operate regardless of national borders, the dialogue between private companies and law enforcement agencies in the EU should evolve from rare encounters to business-as-usual. The Black Wallet Project has observed that law enforcement agencies need a deeper understanding of the products and services of PSPs, whereas PSPs seem to need assistance in providing qualitative STRs. This can be remedied through enhanced communication and cooperative education.

Finally, despite the differences between the private sector and authorities, the safety of our region exist remains a perennial and common goal. Therefore, we need to work together in order to create and sustain a safe environment for the people and for their businesses.

Sources

European Banking Authority, Final Guidelines, 26.6.2017.
https://eba.europa.eu/sites/default/documents/files/documents/10180/1890686/66ec16d9-0c02-428b-a294-ad1e3d659e70/Final%20Guidelines%20on%20Risk%20Factors%20(JC%202017%2037).pdf

Financial Action Task Force, National Money Laundering and Terrorist Financing Risk Assessment, 2013.
https://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

Financial Action Task Force, Terrorist Financing Risk Assessment Guidance, 2019.
https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf

Europol, Internet Organized Crime Threat Assessment, 2019.
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 2019.
https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf


POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation


Polisen
Swedish Police